LAW FIRM OF NAREN THAPPETA
Patent, Trademark, and Copyright Matters
naren@iphorizons.com

(510) 252-9980 (Phone)
(510) 252-9982 (Fax)

39899 Balentine Drive, #119
Newark, California 94560

August 31, 2000

EK183248816US

Box Patent Application
The Honorable Commissioner of
    Patents and Trademarks
Washington, D.C. 20231

Re: New Non-Provisional U.S. Utility Patent Application
    Appl. No.: Unassigned; Filed: Herewith
    For: "Display Unit Storing and Using A Cryptography Key"
    Inventor : Kobayashi et al.
    Our Ref : GNSS-0019

Sir:

The following documents are forwarded herewith for appropriate action by the U.S. Patent and Trademark Office:

1.   U.S. Utility Patent Application entitled: "Display Unit Storing and Using A Cryptography Key"
and naming as inventor: Kobayashi et al.
The application consisting of:

a. A <u>21 page</u> specification containing:
    (i) one page cover sheet
    (ii) 15 pages of description prior to the claims;
    (iii) 4 pages of claims (17 claims);
    (iv) a one page abstract;

b. 4 sheets of drawings: (Figures 1, 2, 3 and 4);

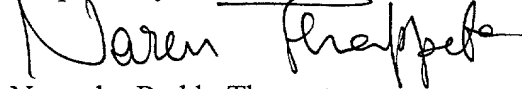Page 1 of 2

2.   An original executed combined declaration and Power of Attorney;

3.   Check No.1251 in the amount of $385.00 to cover the following:
          (i) **$345.00** for the basic filing fee
          (ii) **$40.00** for recordation fees

4.   Recordation Form Cover Sheet (Form PTO-1595);

5.   Assignment to Genesis Microchip, Corp., official recordation and return of which is respectfully requested;

6.   Verified Statement Claiming Small Entity Status; and

7.   A self-addressed stamped post card.

It is respectfully requested that self-addressed stamped postcard, be stamped with the filing date and unofficial application number and returned as soon as possible.

The U.S. Patent and Trademark Office is hereby authorized to charge any fee deficiency, or credit any overpayment, to our Deposit Account No. 20-0674. A duplicate copy of this letter is enclosed.

Respectfully submitted,

Narendra Reddy Thappeta
Attorney for Applicant
Registration No. 41,416

Law Firm of Naren Thappeta
39899 Balentine Drive, # 119
Newark, California 94560
(510) 252-9980
NRT/jka
F:\matters\GNSS\0019\pto cvr filing gnss-19.wpd

In re application of: Kobayashi et al.

Appl. No.: UNASSIGNED

Filed: HEREWITH

For: "Display Unit Storing and Using a
Cryptography Key"

Art Unit: UNASSIGNED

Examiner: UNASSIGNED

Attorney Docket No.: GNSS-0019

VERIFIED STATEMENT CLAIMING SMALL ENTITY STATUS
37 C.F.R. § 1.9 (f) AND 1.27(c) - SMALL BUSINESS CONCERN

I hereby declare that I am:

_____ The owner of a small business concern identified below.

__x__ An official of the small business concern empowered to act on behalf of the concern identified
below.

Name: Genesis Microchip Corp.
Address: 2150 Gold Street, Alviso, CA 95002

I hereby declare that the above identified small business qualifies as a small business concern
as defined in 13 C.F.R. § 121.12. And reproduced in 37 C.F.R. § 1.9(d), for purposes of paying reduced
fees under Section 41(a) and (b) of Title 35 U.S.C. in that the number of employees of the concern,
including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the
number of employees of the business concern is the average over the previous fiscal year of the concern
of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of
the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one
concern controls or has the power to control the other, or a third-party or parties controls or has the
power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the
small business concern identified below with regard to the invention

entitled: "Display Unit Storing and Using a Cryptography Key"

by inventor(s): Kobayashi et al.

described in
_x_ The specification filed herewith
__ Application SC/Serial No. _____ Filed:_____
___ Patent No. _____ Issued _____

If the rights held by the above-identified small business concern are not exclusive, each

individual, concern or organization having rights to the invention is listed below and no rights to the invention are held by any person, other than the inventor, who coupled not qualify as a small business concern under 37 C.F.R. § 1.9 (d) or by any concern which would not qualify as a small business concern under 37 C.F.R. § 1.9(d) or a nonprofit organization under 37 C.F.R. § 1.9(e).

NAME: _____

ADDRESS: _____

[ ] Individual   [ ] Small Business Concern   [ ] Nonprofit Organization

    I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or maintenance fee due after the date on which status as a small business entity is no longer appropriate. (37 C.F.R. § 1.28 (b)).

    I hereby declare that the all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which verified statement is directed.

Name of Person Signing: <u>Mr. Jeffrey Diamond</u>

Title of Person Signing: <u>Chief Operating Officer</u>

Address of Person Signing: <u>2150 Gold Street, Alviso, CA 95002</u>

Signature: <u>Jeffrey Dramond</u>

Date : <u>August   1 5   , 2000</u>

    Note: Separate Verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 C.F.R. § 1.27).

****

Title 37. Code of Federal Regulations, § 1.9(c-f)

(c) An **independent inventor** as used in this chapter means any inventor who (1) has not assigned, granted, conveyed, or licensed, and (2) is under no obligation under contract or law to assign, grant, convey, or license, any rights in the invention to any person who could not likewise be classified as in independent inventor if that person had made the invention, or to any concern which would not qualify as small business concern or a nonprofit organization under this section.

(d) A **small business concern** as used in this chapter means any business concern as defined by the Small business Administration in 13 C.F.R. 121.12. For the convenience of the users of these regulations, that definition states:

121.12 Small Business for paying reduced fees. (a) Pursuant to Pub. L. 97-247, a small business concern for purposes of paying reduced fees under 35 U.S. Code 41(a) and (b) to the Patent and Trademark Office means any business concern (1) whose number of employees, including those of its affiliates, does not exceed 500 persons and (2) which has not assigned, granted, conveyed or licensed, and is under no obligation under contract or law to assign, convey, or license, any rights in the invention to any person who could not be classified as an independent inventor if that person had made the invention, or to any concern which would not qualify as a small business concern or a nonprofit organization under this section. For the purpose of this section concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both. The number of employees of the business concern is the average over the fiscal year of the persons of the fiscal year. Employees are those persons employed on a full-time, part-time or temporary basis during the previous fiscal year

of the concern.

(e) A **nonprofit organization** as used in this chapter means (1) a university or other institution of higher education located in any country; (2) an organization of the type described in section 501(c)(3) of the Internal Revenue Code of 1954 (26 U.S.C. 501(c)(2)) and exempt from taxation under section 501(c)(3) of the Internal Revenue Code of 1954 (26 U.S.C. 501(c)(3)) and exempt from taxation under section 501(a) of the Internal Revenue Code (26 U.S.C. 501(a)); (3) any nonprofit scientific or educational organization qualified under a nonprofit organization statute of a state of this country (35 U.S.C. 201(i)); or (4) any nonprofit organization located in a foreign country which would qualify as a nonprofit organization under paragraphs (e)(2) or (3) of this section if it were located in this country.

(f) A **small entity** as used in this chapter means an **independent inventor**, a **small business concern** or a **nonprofit organization**.

DISPLAY UNIT STORING AND USING A CRYPTOGRAPHY KEY

Inventors

Osamu Kobayashi 1431 Ormsby Drive Sunnyvale, CA 94087 Citizenship: Japan	Ali Noorbakhsh 116 Shadow Creek Court Danville, CA 94506 USA Citizenship: USA
Chia-Lun Hang 15727 Casino Rea Morgan Hill, CA 95037 Citizenship: USA	Jih-Hsien Soong 21712 Columbus Avenue Cupertino, CA 95014 Citizenship: USA
Tzoyao Chan 20237 Marillt Court Saratoga, CA 95070 Citizenship: USA	

Assignee:
    Genesis Microchip Corporation
    2150 Gold Street
    Alviso, CA 95002
    Phone Number: (408)262-6599

Attorney:
    Law Firm of Naren Thappeta
    39899 Balentine Drive, # 119
    Newark, California 94560
    (510) 252-9980 (Phone)
    (510) 252-9982 (Fax)

DISPLAY UNIT STORING AND USING A CRYPTOGRAPHY KEY

Related Applications

The present application is related to and claims priority from U.S. Provisional Application Serial Number 60/184,999, Entitled, "Display Unit Storing and Using a Cryptography Key", Filed on February 25, 2000, which is incorporated into the present application in its entirety.

Background of the Invention

Field of the Invention

The present invention relates to display units used with cryptography technologies, and more specifically to a method and apparatus for storing and using a cryptography key.

Related Art

Display units are often used to receive and display data encoded in a display signal received on a serial communication channel. As used in the present application, display units contain both analog display units (typically based on cathode ray tube technology) and digital display units (typically based on flat panels). The display signal generally contains data representing image frames and synchronization signals (e.g., VSYNC and HSYNC) indicative of the line and frame boundaries.

It may be necessary to implement cryptography applications in display units. In a common cryptography application, underlying data is encrypted at a sending location and

transferred to a receiving location. The encrypted data is then decrypted at a receiving end to recover the original data. Due to the encryption and decryption, an unauthorized third party may be unable to decipher (or even alter) the underlying data when the data is transmitted from the sending location to the receiving location.

5   One common application of cryptography is when a display unit needs to decrypt data encoded in a received display signal. The data is typically encrypted to avoid illegal copying of the data when the display signal is being transmitted. For example, a graphics controller of a computer system may encrypt data representing image frames and send the encrypted data in a serial communication channel, and it may be necessary to decrypt the data in the display unit so

10   that the image frames can be displayed.

Keys are commonly used in cryptography. Examples of such keys include an encryption key used to encrypt data, a decryption key to decrypt the data, and an authentication key to authenticate the source sending data. Details of guidelines (standards) for implementation of cryptography are provided in further detail in a document entitled, "High Bandwidth Digital

15   Content Protection System, Revision 1.0" dated February 17, 2000, and available from Digital Display Working Group (DDWG), which is incorporated in its entirety herewith.

Preventing unauthorized access to keys used in cryptography is often important. For example, the encrypted data can often be decrypted by an unauthorized party if the party has

access to the decryption key. Therefore, what is needed is a method and apparatus which prevents (or substantially discourages) unauthorized access to keys.

Summary of the Invention

An aspect of the present invention provides a secure way of storing and using keys. The keys are stored in encrypted format in a non-volatile memory. The key in the unencrypted form is referred to as an 'unencrypted key' and the key in the encrypted form is referred to as an 'encrypted key'. When the key is to be used, an integrated circuit retrieves the encrypted key from the non-volatile memory, decrypts the key and then uses the decrypted key (which equals the unencrypted key). For example, the integrated circuit may retrieve an encrypted authentication key from the non-volatile memory, decrypt the authentication key, and then use the decrypted authentication key for authentication.

As the keys are stored in encrypted format, an unauthorized user may not be able to decipher the keys by examining the non-volatile memory. In addition, as the key is in encrypted format when retrieved from the non-volatile memory, the key may not be deciphered merely by examining (probing) a bus on which the key is retrieved from the non-volatile memory. Furthermore, as the key is decrypted within an integrated circuit which uses the key, access to the key is further restricted.

A display unit provided according to an aspect of the present invention may thus contain a non-volatile memory (e.g., EEPROM). A master block (external to the display unit) may be

used to generate a key, and the key is provided to the display unit. An encryption circuit encrypts the key according to a protocol and stores resulting encrypted key in the non-volatile memory.

A decryption circuit within the display unit then retrieves the encrypted key, decrypts the key, and uses the decrypted key. The decrypted key may be used for authenticating any subsequently received data. As another example, the decrypted key may be used as a decryption key for decrypting any subsequently received data in a way well known in the relevant arts.

Using the above approach, a component provider may provide a monolithic integrated circuit which contains the encryption and decryption circuits. An OEM (original equipment manufacturer) may provide a key to the encryption circuit, which encrypts the key and stores the encrypted key in a non-volatile memory. When the key is required, the encrypted key is retrieved and decrypted.

Accordingly, a provider may manufacture similar monolithic integrated circuits for many OEMs, and the OEMs may store OEM specific keys in the display units. The keys need not be shared with the providers of the monolithic integrated circuits. As a result, the OEMs may ensure the availability of the key without the fear of comprising security by sharing the keys with the providers.

Therefore, an aspect of the present invention is particularly useful for OEMs as the OEMs may provide keys to the units without having to share the keys with the component providers.

An aspect of the present invention makes it difficult for an unknown third party to access keys as the keys are stored in an encrypted form in a non-volatile memory and the key may be

5   retrieved from the memory only in encrypted form.

Another aspect of the present invention makes it difficult for an unknown third party to access the keys as the key may be available in decrypted form only within the integrated circuits during actual use.

Further features and advantages of the invention, as well as the structure and operation

10   of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawing in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number.

Brief Description of the Drawings

15   The present invention will be described with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a computer system implemented in accordance with the present invention;

Figure 2 is a block diagram the manner in which a key can be stored and used in accordance with the present invention;

Figure 3 is a block diagram illustrating a display unit implemented in accordance with the present invention; and

5   Figure 4 is a flow-chart illustrating a method in accordance with the present invention.

Detailed Description of the Preferred Embodiments

1. Overview and Discussion of the Invention

The present invention is described in the context of a display unit which stores one or more keys in encrypted format ("encrypted key") in a non-volatile memory. When the key is to

10 be used, an integrated circuit retrieves the encrypted key from the non-volatile memory, decrypts the key and then uses the decrypted key. For example, the integrated circuit may retrieve an encrypted authentication key from the non-volatile memory, decrypt the authentication key, and then use the authentication key for authentication.

As the keys are stored in encrypted format, an unauthorized user may not be able to

15 decipher the keys by examining the non-volatile memory. In addition, as the key is in encrypted format when retrieved from the non-volatile memory, the key may not be deciphered merely by examining (probing) a bus on which the key is retrieved from the non-volatile memory. Furthermore, as the key is decrypted within an integrated circuit which uses the key, access to the key is further restricted.

The present invention is described below with reference to several examples for illustration. One skilled in the relevant art, however, will readily recognize that the invention can be practiced in other environments without one or more of the specific details, or with other methods, etc. In other instances, well-known structures or operations are not shown in detail to avoid obscuring the invention.

2. Example Environment

In general, the present invention can be implemented in any display unit, for example, used in conjunction with computer systems, DVD Players, HDTV televisions, etc. However, the invention is described below with reference to computer systems for illustration. A computer system may be one of, without limitation, lap-top and desk-top personal computer systems, work-stations, special purpose computer systems, general purpose computer systems, network computers, and many others. The invention may be implemented in hardware, software, firmware, or combination of the like.

Figure 1 is a block diagram of computer system 100 illustrating an example environment in which the present invention can be implemented. Computer system 100 includes central processing unit (CPU) 110, random access memory (RAM) 120, one or more peripherals 130, graphics controller 160, and digital display unit 170. CPU 110, RAM 120 and graphics controller 160 are typically packaged in a single unit, and such a unit is referred to as source 199 as the unit generates and transmits a sequence of symbols on a serial communication channel.

All the components in graphics source 199 of computer system 100 communicate over bus 150, which can in reality include several physical buses connected by appropriate interfaces.

RAM 120 stores data representing commands and possibly pixel data elements representing a source image. CPU 110 executes commands stored in RAM 120, and causes

5   different commands and pixel data elements to be transferred to graphics controller 160. Peripherals 130 can include storage components such as hard-drives or removable drives (e.g., DVD drive, floppy-drives). Peripherals 130 can be used to store commands and/or data which enable computer system 100 to operate in accordance with the present invention. By executing the stored commands, CPU 110 provides the electrical and control signals to coordinate and

10   control the operation of various components in graphics source 199.

Graphics controller 160 receives data/commands from CPU 110, and generates pixel data elements representative of source images to be displayed on digital display unit. Graphics controller 160 then encodes the data as symbols in a serial communication channel. The symbols may be sent in an encrypted format. The resulting signal ("display signal") may contain

15   synchronization signals also in addition to the data. The display signal may be transferred according to standards such as Digital Flat Panel (DFP) and Digital Video Interface (DVI) well known in the relevant arts.

Display unit 170 may receive a display signal in TMDS format from graphics controller 160, and displays the source images encoded in the display signal. As the symbols (data) may

be encoded in an encrypted format, display unit 170 first decrypts the symbols to recover the pixel data elements representing a source image. The corresponding source images are then displayed. The display unit may provide for authentication also. As is well known, decryption and authentication type acts require keys.

5   As described below in further detail, the present invention enables the keys to be stored in a non-volatile memory while minimizing the risk that an unknown third party can access the keys. The components of the digital display unit as relevant to the present invention are described below in further detail. The details of display unit are then described in further detail. For further details on the operation of the components, the reader is referred to the co-pending

10   application serial Number: 09/406,332; Filing Date: September 27, 1999, entitled, "Receiver to Recover Data Encoded in a Serial Communication Channel", which is incorporated in its entirety herewith.

3. Use of Key

        Figure 2 is a block diagram of apparatus 200 illustrating the manner in which keys are

15   stored and used in accordance with the present invention. Apparatus is shown containing printed circuit board (PCB) 299 and master block 210. PCB 299 (or parts thereof) are referred to as components which are provided by component providers such as Genesis Microchip Corporation (the assignee of the present application). OEMs (original equipment manufacturers) such as Sony Corporation and Compaq Corporation integrate such components into units such as display

20   units.

In operation, an OEM uses master block 210 to provide keys ("encrypted keys") to printed circuit board (PCB) 299. The keys may be generated either internal or external to master block 210, and may be provided in an unencrypted format. The key may be provided in unencrypted form to PCB 299 using I^{2}C protocol well known in the relevant arts. As described

5   below in further detail, PCB 299 stores the key(s) in an encrypted form/format ("encrypted key") in a non-volatile memory, and decrypts the keys when required for use.

PCB 200 may contain monolithic integrated circuit 201, pin header 211, EEPROM 250, micro-controller 260 and DVI (digital video interface) connector 270. Integrated circuit 201 is in turn shown to contain RAM 220, key encryption circuit 230, port 240, the High-bandwidth

10   Digital Content Protection (HDCP) engine 290 (containing key decryption circuit 295 and data decryption circuit 296), and receiver 285. Each component is described below in further detail.

Pin header 211 may contain two pins (consistent with I^{2}C protocol) and provides the physical interface to communicate with master block 210. The data received by pin header 211 includes keys which are stored and used in accordance with various aspects of the present

15   invention.

Port 240 receives an unencrypted key and places the key in random access memory (RAM) 220, which can also be implemented as multiple registers. Key encryption circuit 230 encrypts the key according to an encryption protocol and stores the encrypted key in RAM 280. The encrypted key can be written directly into serial EEPROM 250 by key check and encrypt

230 if such a feature is available. Alternatively, master block 210 may retrieve the encrypted key from RAM 280, and write the encrypted key into serial EEPROM 250.

One problem with the above embodiment is that an unauthorized third party may retrieve the encrypted key multiple times and attempt to decipher the unencrypted key. To discourage
5 such attempts, support for multiple encryption/decryption protocols (for encrypting the keys) may be provided within integrated circuit 201, and the keys may be encrypted according to one of the protocols. The OEM may specify the specific protocol by using appropriate commands. The data indicating the specific protocol may also be stored thereafter in serial EEPROM 250 to facilitate later decryption by HDCP engine 290.

10 As a further deterrent against unauthorized deciphering of the keys, the OEM may be required to provide a secret key (generated based on a protocol provided by the component manufacturer), and the appropriate encrypted key may be provided only if the secret key is deemed to authenticate the OEM. As a result, third parties may be unable to access or decipher the keys stored and used in accordance with the present invention.

15 Using the noted approaches of above, several keys may be written into EEPROM 250. For example, the keys may include authentication key and a decryption key. The manner in which these keys are used is described below in further detail.

DVI connector 270 may receive any cryptography related commands from graphics controller using, for example, I²C protocol on path 272. As an illustration, DVI connector 270 may receive a request to authenticate along with any necessary parameters. The authentication request is passed to HDCP engine 290 in integrated circuit 201. HDCP engine 290 retrieves the

5   encrypted authentication key from serial EEPROM 250 via RAM 220, and decrypts it according to a corresponding decryption algorithm.

The decrypted authentication key can be used to provide a response to the authentication request. Once the authentication key is decrypted, the response to the authentication can be generated in a known way. Path 272 may be used to implement the communication for the

10   authentication.

DVI connector 270 is shown connected to two paths, I²C path 272 and display signal path 271. I²C path 272 may be used to send and receive various security related commands (e.g., authentication sequence as noted above) using the I²C well known in the relevant arts. DVI connector 270 may receive data in encrypted format, for example, from the graphics controller

15   in TMDS format on path 271. The signals are forwarded to receiver 285 in integrated circuit 201. Receiver 285 recovers the data representing the encrypted pixel data element values and forwards the recovered data to HDCP engine 290, which is shown containing data decrypt block 296 and key decrypt block 295.

Key decryption block 295 receives the decryption key from serial EEPROM 250 via RAM 220, and decrypts the encrypted decryption key according to a decryption algorithm consistent with the encryption algorithm with which the decryption key may have been earlier encrypted. The decrypted key is forwarded to data decrypt block 296. External micro 260

5   coordinates and controls different components in printed circuit board 299.

It should be noted that the decrypted keys are available only in integrated circuit 201, that too only when the circuit is operational. Accordingly, unauthorized third parties may be unable to access the decrypted key even by snooping the buses from which the keys are retrieved from non-volatile serial EEPROM 250. As a result, the keys used in accordance with the present

10   invention may be prone less to unauthorized accesses.

Data decryption block 296 decrypts the data recovered by receiver 285. As the resulting decrypted data represents pixel data elements forming image frames, a display unit may display the images, for example, as described below.

4. Example Display unit

15   Figure 3 is a block diagram illustrating an example embodiment of display unit 170. Display unit 170 is shown containing printed circuit board 299, display interface 330, and display screen 350. As described above, printed circuit board 299 receives encrypted pixel data elements from a graphics controller on path 271, and generates the decrypted data on path 297.

Display interface 330 receives the decrypted data containing pixel data elements on path 297. Display interface 330 is implemented consistent with the interface requirements of display screen 350. Display screen 350 can be an analog display screen scanned using CRT technology or a flat panel. Alternatively, display screen 350 may be a digital display screen based on flat

5 panel monitor. Display interface 330 generates the corresponding display signals to cause the images represented by the pixel data elements to be displayed on display screen 350.

Thus, the present invention provides a display unit which enables keys to be stored and used while minimizing the risk of unauthorized access of the keys. A method in accordance with the present invention may be summarized as following.

5. Method

10

Figure 4 is a flow chart illustrating a method in accordance with the present invention. The method is described with reference to display unit 170 for illustration. The method starts in step 401 in which control passes to step 410. In step 410, display unit 170 receives a key.

In step 420, display unit 170 decrypts the key according to an encryption protocol. As
15 noted above, display unit 170 may be designed to encrypt the key using one of several encryption protocols. In step 430, display unit 170 stores the encrypted key in a non-volatile memory. The non-volatile memory may be located within display unit 170 as described above. In addition, the memory may be implemented with components such as entire memory modules (e.g., EEPROM) or using a small memory units such as registers.

In step 440, display unit 170 may retrieve the encrypted key when needed. A need arises according to the specific purpose for which the key is designed for. For example, if the key is used for encryption, the key is retrieved prior to decryption of the corresponding data. In step 460, display unit 170 decrypts the key consistent with the encryption protocol used above. In

5   step 470, display unit 170 uses (e.g., for authentication or decryption of data) the decrypted key. Display unit 170 may retrieve the keys any number of times as indicated by the loop shown in Figure 4.

Thus, a display unit provided in accordance with the present invention may store any keys in an encrypted form in a non-volatile memory, and decrypt the key only when actually required for use. As a result, the keys may not be easily deciphered and accessed by an unauthorized third party. In addition, it should be understood that steps 410-430 are performed usually by an OEM at the time of assembling the display units, and the loop of steps 440-470 is performed when a end user uses the display unit later.

6. Conclusion

15   While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What is claimed is:

1   1. A method of using an unencrypted key, said method comprising:

2   encrypting said unencrypted key according to an encryption protocol to generate an

3   encrypted key;

4   storing said encrypted key in a non-volatile memory;

5   retrieving said encrypted key into an integrated circuit when said unencrypted key is

6   required for use;

7   decrypting said encrypted key in said integrated circuit to generate said unencrypted key;

8   and

9   using said unencrypted key.

1   2. The method of claim 1, wherein said unencrypted key is used within said integrated

2   circuit.

1   3. The method of claim 2, wherein said unencrypted key comprises an authentication key

2   and said using comprises authenticating a source of data.

1   4. The method of claim 2, wherein said unencrypted key comprises a decryption key and

2   said using comprises decrypting data.

1   5. A method of using a unencrypted key in a display unit, said method comprising:

2   receiving said unencrypted key in said display unit;

3   encrypting said key according to an encryption protocol to generate an encrypted key;

4   storing said encrypted key in a non-volatile memory contained within said display unit;

5   retrieving said key into an integrated circuit when said key is required for use, wherein

6   said integrated circuit is contained within said display unit;

7   decrypting said key in said integrated circuit; and

8   using said key.

1   6. The method of claim 5, wherein said display unit comprises an analog display unit.

1   7. The method of claim 5, wherein said display unit comprises a digital display unit.

1   8. The method of claim 5, further comprising receiving a display signal containing a

2   plurality of pixel data elements in an encrypted format, wherein decryption of said plurality of

3   pixel data elements requires said unencrypted key, wherein said unencrypted key is used to

4   decrypt said plurality of pixel data elements.

1   9. The method of claim 5, further comprising authenticating a source of data, wherein

2   said authenticating is performed using said unencrypted key based on data sent and received on

3   a path connected to said display unit.

1   10. The method of claim 9, wherein said path is implemented using I^2C protocol.

1   11. The method of claim 5, wherein a master block external to said display unit sends

2   said unencrypted key, said method further comprising sending said encrypted key to said master

3   block, wherein said mater block stores said encrypted key in said non-volatile memory.

1   12. A display circuit for use in a display unit, said display circuit comprising:

2   a non-volatile memory storing a encrypted key, wherein said encrypted key is generated

3   from an unencrypted key according to an encryption protocol;

4   an integrated circuit coupled to said non-volatile memory, said integrated circuit receiving

5   said key in encrypted form and decrypting said key to generate a decrypted key, said integrated

6   circuit using said decrypted key.

1   13. The display circuit of claim 12, wherein said integrated circuit comprises a key

2   encryption circuit receiving said unencrypted key, said key encryption circuit generating said

3   encrypted key from said unencrypted key according to said encryption protocol.

1   14. The display circuit of claim 13, wherein said integrated circuit further comprises:

2   a memory receiving said encrypted key; and

3   a port coupled to said memory, said port receiving said encrypted key from said memory

4   and sending said encrypted key to a master block, wherein said master block stores said

5   encrypted key in said non-volatile memory.

1   15. The display circuit of claim 13, wherein said integrated circuit further comprises a

2   key decryption circuit receiving said encrypted key, and generating said decrypted key according

3   to said encryption protocol.

1   16. The display circuit of claim 15, further comprising:

2   a receiver receiving a plurality of digital data elements encoded in a display signal,

3   wherein said digital data elements represent a plurality of pixel data elements in an encrypted

4   form, said plurality of pixel data elements representing an image; and

5   a data decryption circuit receiving said plurality of digital data elements and generating

6   said plurality of pixel data elements,

7   wherein said image is generated on a display screen based on said plurality of pixel data

8   elements.

1   17. The display circuit of claim 16, wherein said display signal is received according to

2   TMDS format.

Abstract

Display Unit Storing and Using a Cryptography Key

Keys (e.g., decryption key, authentication key) are stored in a non-volatile memory of a display unit. The keys are retrieved in encrypted form into an integrated circuit. The integrated

5   circuit decrypts the keys and uses the keys. As the keys are available in decrypted form only within the integrated circuit and potentially only during use, the keys may not be available to unauthorized third parties.
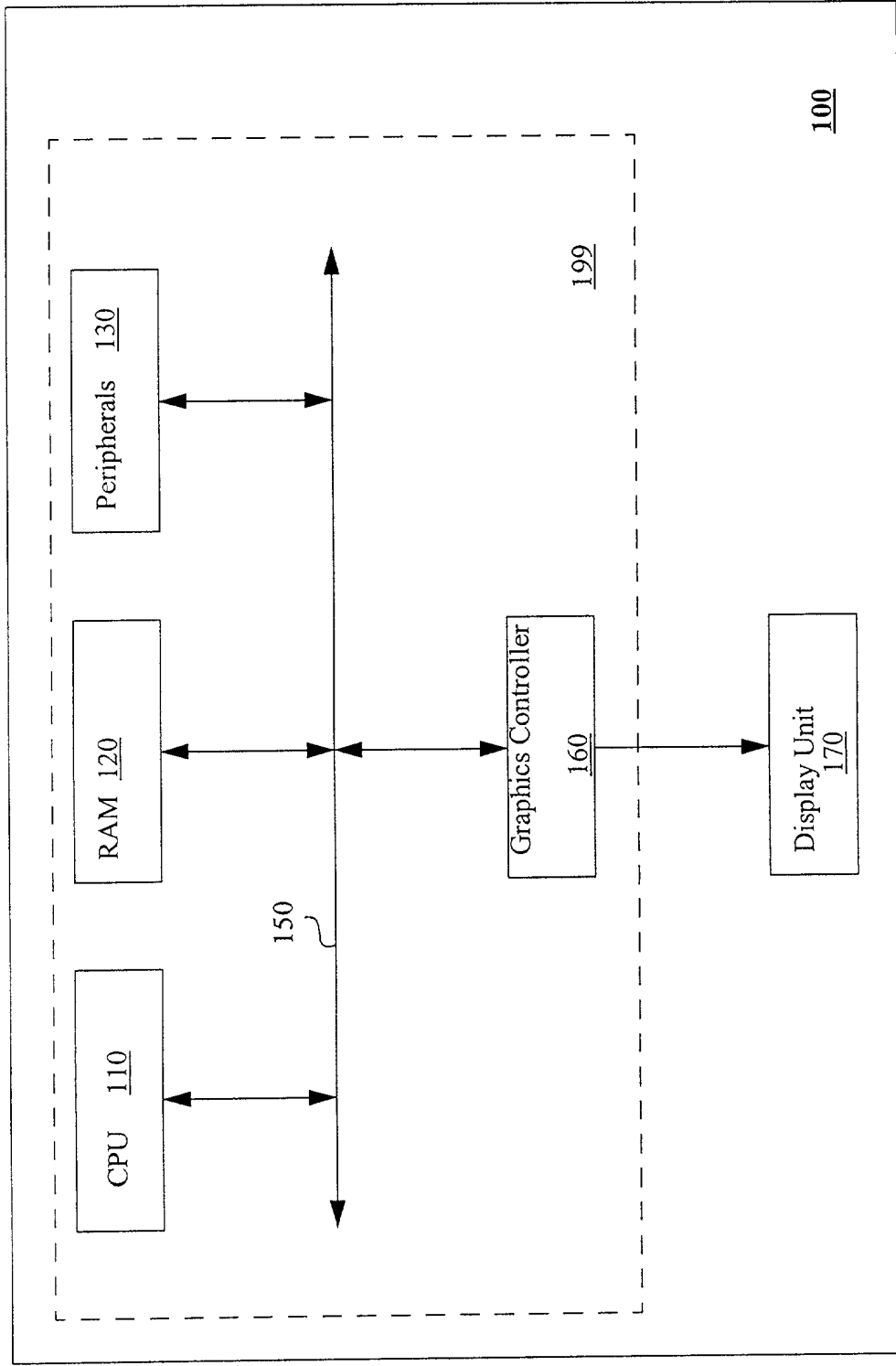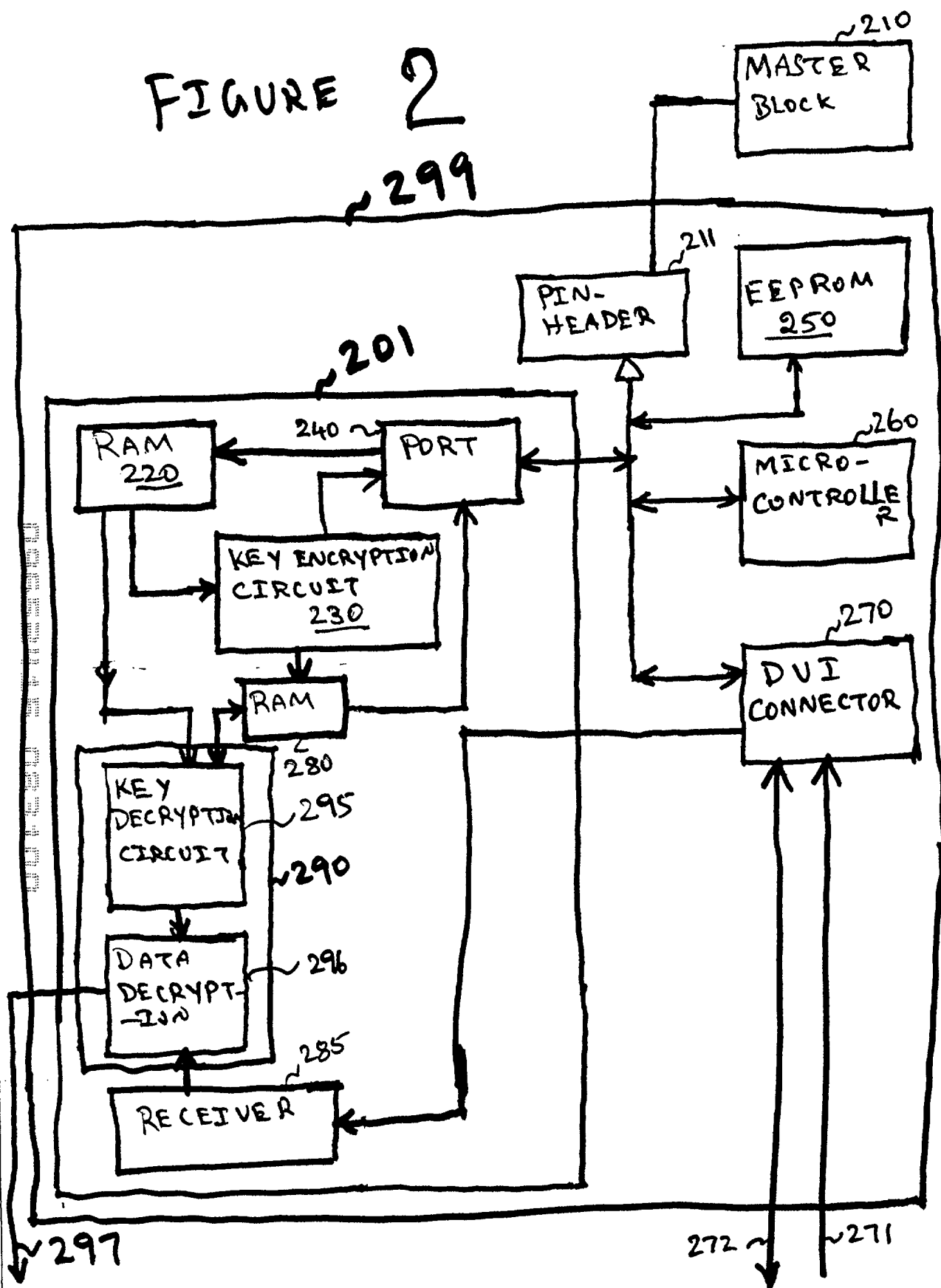
F:\matters\GNSS\0019\regular patent gnss-19.wpd

Peripherals 130

RAM 120

CPU 110

150

199

Graphics Controller
160

Display Unit
170

100

Figure 1

FIGURE 2

MASTER Block ~210

PIN-HEADER ~211

EEPROM 250

MICRO-CONTROLLER ~260

DUI CONNECTOR ~270

~299

~201

RAM 220

240 ~

PORT

KEY ENCRYPTION CIRCUIT 230

RAM ~280

KEY DECRYPTION CIRCUIT ~290 ~295

DATA DECRYPT-ION ~296

RECEIVER ~285

~297

272 ~   ~271

FIGURE 3

I^{2}C 272

271

FROM TMDS TRANSMITTER

PRINTED CIRCUIT BOARD 299

297

DISPLAY INTERFACE 330

DISPLAY SCREEN 350

170

●   ●

Begin ⟩ 401

Receive a key — 410

Encrypt the received key according to an encryption protocol — 420

Store the encrypted key in a non-volatile memory — 430

Retrieve the encrypted key when needed — 440

Decrypt the key — 460

Use the key — 470

Destroy the key — 480

401 **Figure 4**

Combined Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled, "Display Unit Storing and Using a Cryptography Key" the specification of which is attached hereto unless the following box is checked:

☐ was filed on_____;
  as United States Application Number or PCT International Application Number_____; and
  was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information that is material to patentability as defined in 37 C.F.R. § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)   Priority Claimed

                           [ ] Yes [x] No

_____ _____ _____
(Application No.)   (Country)   (Day/Month/Year Filed)

                           [ ] Yes [x] No

_____ _____ _____
(Application No.)   (Country)   (Day/Month/Year Filed)

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

60/184,999_____ February 25, 2000_____

(Application No.)   (Filing Date)

_____ _____
(Application No.)   (Filing Date)

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information that is material to patentability as defined in 37 C.F.R. § 1.56 that became available between the filing date of the prior application and the national or PCT International filing date of this application.

_____ _____ _____
(Application No.)   (Filing Date)   (Status - patented, pending, abandoned)

_____ _____ _____
(Application No.)   (Filing Date)   (Status - patented, pending, abandoned)

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

    Narendra Reddy Thappeta, Esq., Registration Number: 41,416

Send Correspondence to:
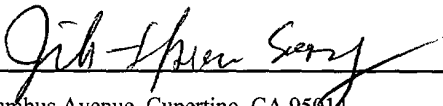
LAW FIRM OF NAREN THAPPETA   Phone Number: (510) 252-9980
39899 Balentine Drive, #119   Fax Number: (510) 252-9982
Newark, California 94560

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of First inventor: Osamu Kobayashi	
Inventor's signature	Date: August 8, 2000
Residence: 1431 Ormsby Drive, Sunnyvale, CA 94087	
Citizenship: Japan	
Post Office Address: Same as above	

Full name of joint inventor: Ali Noorbakhsh	
Inventor's signature	Date: August 8, 2000
Residence: 116 Shadow Creek Court, Danville, CA 94506 USA	
Citizenship: U.S.A.	
Post Office Address: Same as above	

Full name of joint inventor: Chia-Lun Hang	
Inventor's signature	Date: August 11, 2000
Residence: 15727 Casino Rea, Morgan Hill, CA 95037	
Citizenship: U.S.A.	
Post Office Address: Same as above	

Full name of joint inventor: Jih-Hsien Soong

Inventor's signature	Date
Jih-Hsien Soong	August 8 , 2000

Residence: 21712 Columbus Avenue, Cupertino, CA 95014

Citizenship: U.S.A.

Post Office Address: Same as above

Full name of joint inventor: Tzoyao Chan

Inventor's signature	Date
Tzoyao Chan	August 8 , 2000

Residence: 20237 Marillt Court, Saratoga, CA 95070

Citizenship: U.S.A.

Post Office Address: Same as above

37 § C.F.R. 1.56 Duty to Disclose Information Material to Patentability

(a)   A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of an evaluates the teaching of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office; Which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of a claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of an existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner described by sections 1.97(b)-(d) and 1.98. However no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applications to carefully examine:

   (1)   prior art cited in search reports of a foreign patent office in a counterpart application, and

   (2)   the closest information over which individual associated with the filing or prosecution of a patent application believe any pending claim patentability defines, to make sure that any material information contained therein is disclosed to the Office.

(b)   Under this section, information is material to patentability when is it not cumulative to information already of record of being made of record in the application, and

   (1)   It establishes, by itself or in combination with other information, a prima facie case of un patentability of a claim; or

   (2)   It refutes, or is inconsistent with, a position the application takes in:

      (I)   opposing an argument of un patentability relied on by the Office, or

      (ii)   Asserting an argument of patentability.

A prima facie case of un patentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term of the claim its broadest reasonable construction consistent with the specification, and before any considerations given to evidence which may be submitted in an attempt to establish a contrary conclusion of a patentability.

(c)   Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

   (1)   Each inventor named in the application;

   (2)   Each attorney or agent who prepares or procures the application; and

   (3)   Every other person who is substantively involved in the preparation of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

   (4)   Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent or inventor.

F:\matters\GNSS\0019\dec and poa gnss-19.wpd